AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A system comprising:

a controller module comprising instructions for controlling a first component, wherein the controller module is provided dynamically;

a storage system capable of storing a set of semantic programming that enables a second component to understand the semantics of a set of universal interfaces associated with the controller module; and

~~a~~ the second component with a security system that interacts with the controller module to implement a security protocol before the second component can control the first component based on executing the instructions in the controller module, wherein the controller module provides secure control of communications between the first component and the second component, and wherein the security system decrypts an encrypted controller module to perform a portion of the security protocol, the second component ~~controls~~ controlling the first component based upon the execution of the instructions in the controller module without the second component having prior knowledge of the first component, wherein the stored set of semantic programming enables secure ad hoc interaction between the first and second components.

2. (Original) The system as set forth in claim 1 wherein a portion of the instructions in the controller module comprises authentication instructions which when executed by the second component cause the second component to send

authentication information to the first component to perform a portion of the security protocol.

3. (Original) The system as set forth in claim 2 wherein the authentication information is associated with an operator of the second component, the first component authenticates the operator using the authentication information to perform another portion of the security protocol.

4. (Original) The system as set forth in claim 2 wherein the first component authenticates the second component using the authentication information to perform another portion of the security protocol, wherein upon unsuccessful authentication the first component rejects messages from the second component and upon successful authentication the first component accepts the messages from the second component, the messages being associated with controlling the first component.

5. (Original) The system as set forth in claim 2 wherein the first component authenticates each of a plurality of messages received from the second component, the messages being associated with controlling the first component, wherein upon unsuccessful authentication of at least one of the messages the first component rejects the at least one message and upon successful authentication of another at least one of the messages the first component accepts the other at least one message from the second component.

6 (Canceled).

7. (Previously presented) The system as set forth in claim 1 wherein the security system uses a cryptographic key associated with one of the first

component, the second component and a third component to decrypt the encrypted controller module.

8. (Original) The system as set forth in claim 1 wherein the security system authenticates the controller module using at least one of a digital certificate, a public key and a shared secret to perform a portion of the security protocol.

9. (Original) The system as set forth in claim 1 wherein the security system rejects the controller module upon determining that a cryptographic signature associated with the controller module is not associated with a trusted component to perform a portion of the security protocol.

10. (Original) The system as set forth in claim 1 wherein the controller module is encrypted using a cryptographic key from one of the first component, the second component and a third component.

11. (Original) The system as set forth in claim 1 wherein the controller module comprises a cryptographic signature associated with at least one of the first component and one or more third components.

12. (Currently amended) A method comprising:

providing a controller module comprising instructions for controlling a first component, wherein the controller module is provided dynamically;

storing a set of semantic programming that enables a second component to understand the semantics of a set of universal interfaces associated with the controller module; and interacting with the controller module to implement a security protocol before ~~a~~the second component can control the first component based on executing the instructions in the controller module, wherein the controller module provides secure control of communications between the first component and the second component without the second component having prior knowledge of the first component, wherein the stored set of semantic programming enables secure ad hoc interaction between the first and second components;

wherein the interacting with the controller module to implement the security protocol further comprises:

decrypting an encrypted controller module to perform a portion of the security protocol, and

controlling the first component based upon the execution of the instructions in the controller module.

13. (Original) The method as set forth in claim 12 wherein the interacting with the controller module to implement the security protocol further comprises:

executing a portion of the instructions in the controller module that comprises authentication instructions;

sending authentication information from the second component to the first component to perform a portion of the security protocol based on the executed authentication instructions.

14. (Original) The method as set forth in claim 13 further comprising authenticating an operator of the second component using the authentication information to perform another portion of the security protocol.

15. (Original) The method as set forth in claim 13 further comprising:

authenticating the second component using the authentication information to perform another portion of the security protocol; and rejecting messages from the second component upon unsuccessful authentication and accepting the messages from the second component upon successful authentication, the messages associated with controlling the first component.

16. (Original) The method as set forth in claim 13 further comprising:

authenticating each of a plurality of messages from the second component, the messages associated with controlling the first component; and

rejecting at least one of the messages from the second component upon unsuccessful authentication of the at least one message and accepting another at least one of the messages upon successful authentication of the other at least one message.

17 (Canceled).

18. (Previously presented) The method as set forth in claim 12 further comprising using a cryptographic key associated with one of the first component, the second component and a third component to decrypt the encrypted controller module.

19. (Original) The method as set forth in claim 12 further comprising authenticating the controller module using at least one of a digital certificate, a public key and a shared secret to perform a portion of the security protocol.

20. (Original) The method as set forth in claim 12 further comprising rejecting the controller module upon determining that a cryptographic signature associated with the controller module is not associated with a trusted component to perform a portion of the security protocol.

21. (Original) The method as set forth in claim 12 further comprising encrypting the controller module using a cryptographic key from one of the first component, the second component and a third component.

22. (Original) The method as set forth in claim 12 wherein the controller module comprises a cryptographic signature associated with at least one of the first component and one or more third components.

23. (Currently amended) A computer-readable medium having stored thereon instructions, which when executed by at least one processor, causes the processor to perform:

providing a controller module comprising instructions for controlling a first component, wherein the controller module is provided dynamically;

storing a set of semantic programming that enables a second component to understand the semantics of a set of universal interfaces associated with the controller module; and

interacting with the controller module to implement a security protocol before ~~a~~the second component can control the first component based on executing the instructions in the controller module, wherein the controller module provides secure control of communications between the first component and the second component without the second component having prior knowledge of the first component, wherein the stored set of semantic programming enables secure ad hoc interaction between the first and second components;

wherein the interacting with the controller module to implement the security protocol further comprises:

decrypting an encrypted controller module to perform a portion of the security protocol, and controlling the first component based upon the execution of the instructions in the controller module.

24. (Original) The medium as set forth in claim 23 wherein the interacting with the controller module to implement the security protocol further comprises:

executing a portion of the instructions in the controller module that comprises authentication instructions;

sending authentication information from the second component to the first component to perform a portion of the security protocol based on the executed authentication instructions.

25. (Original) The medium as set forth in claim 24 further comprising authenticating an operator of the second component using the authentication information to perform another portion of the security protocol.

26. (Original) The medium as set forth in claim 24 further comprising:

authenticating the second component using the authentication information to perform another portion of the security protocol; and

rejecting messages from the second component upon unsuccessful authentication and accepting the messages from the second component upon successful authentication, the messages associated with controlling the first component.

27. (Original) The medium as set forth in claim 24 further comprising:

authenticating each of a plurality of messages from the second component, the messages associated with controlling the first component; and

rejecting at least one of the messages from the second component upon unsuccessful authentication of the at least one message and accepting another at least one of the messages upon successful authentication of the other at least one message.

28 (Canceled).

29. (Previously presented) The medium as set forth in claim 23 further comprising using a cryptographic key associated with one of the first component, the second component and a third component to decrypt the encrypted controller module.

30. (Original) The medium as set forth in claim 23 further comprising authenticating the controller module using at least one of a digital certificate, a public key and a shared secret to perform a portion of the security protocol.

31. (Original) The medium as set forth in claim 23 further comprising rejecting the controller module upon determining that a cryptographic signature associated with the controller module is not associated with a trusted component to perform a portion of the security protocol.

32. (Original) The medium as set forth in claim 23 further comprising encrypting the controller module using a cryptographic key from one of the first component, the second component and a third component.

33. (Original) The medium as set forth in claim 23 wherein the controller module comprises a cryptographic signature associated with at least one of the first component and one or more third components.